

Knowledge Superiority and Expeditionary Maneuver Warfare



Knowledge Superiority and Expeditionary Maneuver Warfare

Information technology will provide a key foundation for the effort to transform U.S. armed forces for the 21st Century...[It] offers U.S. forces the potential of conducting joint operations more effectively, with smaller forces and fewer weapons systems.

2001 Quadrennial Defense Review

As modern weaponry and advanced naval technologies become more common internationally, even large and sophisticated expeditionary forces will find themselves potentially vulnerable to low-end “asymmetric” threats, particularly when wielded for area denial in constricted littoral waters. With “assured access” a key element of Naval Vision 2020 and given the Navy-Marine Corps emphasis on “influencing events on land... from the sea,” an effective area-denial strategy that thwarts access to the littoral could seriously disrupt many expeditionary concepts of operation. Thus, despite overwhelming resources and demonstrably superior military technology, the specter of embarrassing setbacks continues to haunt U.S. planners. Likely threats run the gamut from adversary submarines, to ballistic missiles, to surface combatants, to a wide array of aircraft, to cruise missiles fired from ships, submarines, aircraft, or shore emplacements, to mines, to shore batteries, to small boats and craft, and a host of others. Each of these capabilities, singly or in concert, has the potential to deny or delay access to the littoral.



With local superiority in weaponry no longer guaranteed; with potential adversaries increasingly well-provided with advanced sensor and surveillance technologies; and with diminishing tolerance for losses, eking out a tactical advantage over these and other asymmetric threats is a defining challenge for naval expeditionary forces today. In response, the Navy-Marine Corps team depends heavily on exploiting two historic military principles: maneuver warfare and knowledge superiority.

In fact, today's fast-moving maneuver warfare demands a greater knowledge advantage over potential adversaries than ever before, and it is the function of the command and control system and an accompanying infrastructure for intelligence, surveillance, and reconnaissance (ISR) to provide it.

New Demands on C4ISR in Maneuver Warfare

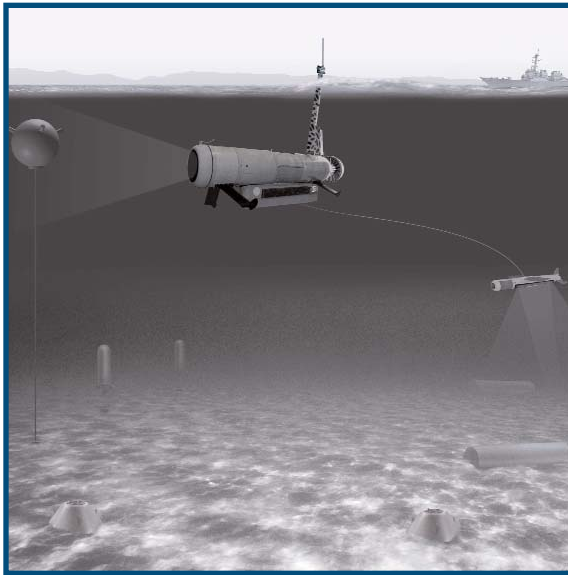
As the Navy and Marine Corps retool their concepts of operations for expeditionary warfare in the 21st century, two central ideas stand out: Operational Maneuver From the Sea (OMFTS) and Ship-to-Objective Maneuver (STOM). In OMFTS, the Corps' long tradition of amphibious opera-



tions is married to the principles of maneuver warfare in a new approach to sea-borne assault, in which rapidly-moving air-ground forces use the sea as a maneuver space to set up attacks along multiple axes toward objectives inland. In STOM, the movement from amphibious ships offshore is carried out in one smooth progression without pausing at the shoreline to create a “beachhead” or lodgement for the support of follow-on elements. In both, the emphasis is on surprise, dispersal, fast, mutually-coordinated attacks, and self-sustaining “just-in-time” logistics – all intended to keep an adversary off-balance and foreclose his tactical options. Incorporating offshore Navy strike or land-attack capabilities, the naval amphibious force constitutes a powerful, first-in, joint-force enabler that “springs the door” for larger follow-on echelons and holds it open to ensure their safe arrival.



No other form of modern conflict demands more robust, flexible, and pervasive command and control than naval expeditionary warfare, with its constantly shifting evolution of land-attack fires, force protection, OMFTS, and STOM. And with “preparation of the battlespace” more important than ever for creating surprise and seizing the tactical advantage, ISR will play a crucial and increasing role in the revolution that is revamping expeditionary warfighting today.



Moreover, with naval forces spread more thinly over a multiplicity of missions and dispersed over larger geographical areas, command/control is forced to play an escalating role as a “force multiplier.” For example, as amphibious ready groups (ARGs) are driven more frequently into “split-ARG” operations, in which small numbers of ships – or even individual units – are called on to operate alone, only a robust command and communications infrastructure will enable the mutual support and force protection hitherto gained by operating together and contiguously. And to counter the threat of enemy mining along potential lines of approach, only the most comprehensive ISR capabilities will develop the environmental and threat information needed to maneuver around dangerous waters and avoid untenable landing zones.

Thus, the whole “operational art” of command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) is stressed to the utmost by expeditionary maneuver warfare – and particularly by OMFTS. The need to coordinate fast-moving, mutually-supportive attacks along multiple axes by dispersed and relatively independent forces itself creates a difficult challenge. In consonance with the Joint Vision 2020 goals of precision engagement and focused logistics, there is also the requirement for organizing supporting fires and directing the delivery of fuel, ammunition, and supplies to the point of the spear in near-real time.

Furthermore, with so much of the success of maneuver warfare dependent on the exploitation of a superior knowledge of the adversary, the battlespace, and fleeting enemy vulnerabilities, ISR capabilities will be severely challenged. Indeed, modern naval forces will depend increasingly on establishing an “information advantage” over potential opponents not as well equipped with sensors, computers, and communications. In its essentials, this central role of information hearkens back to the observation of the Duke of Wellington, who said in simpler times that, “All the business of war, and indeed all the business of life, is to find out what you don’t know from what you do; that’s what I called ‘guessing what was at the other side of the hill.’

Elements of Network-Centric Warfare

During the last decade, the Navy and Marine Corps have begun to engineer a sweeping transition from the “platform-centric” force of the recent past to the “network-centric” force of the future. The central theme of network-centric warfare (NCW) is the use of mutually-shared information and a common tactical picture to enable the coherent employment of the Navy/Marine Corps force – indeed, any joint force – as a single synergistic entity that derives its power from the strong networking of geographically dispersed elements. Essentially, this transformation seeks to harness the explosion of information technology in industry to give decision-makers at all levels timely access to more relevant information, improve their overall situational awareness, and facilitate the ability to plan, coordinate, and execute “effects-based” combat operations.



Since the overall effectiveness of a networked force will increase geometrically with the number of well-informed participants and the currency and accuracy of their shared tactical information, NCW promises extraordinary “force-multiplier” advantages. Achieving knowledge superiority over the enemy will shorten decision cycles and allow friendly elements to “self-synchronize” their actions “from the bottom up” in accordance with a

general statement of intent and without detailed and voluminous orders from above. In particular, NCW concepts dovetail very closely with the C4ISR requirements of OMFTS and STOM.

This knowledge superiority – encompassing not only a clear view of the tactical situation, but also an in-depth understanding of the adversary’s order of battle, infrastructure, history, and value systems – will enable the network-centric force to concentrate on achieving optimum effects, vice attrition. Thus, instead of attacking the enemy’s numbers, “knowledge-based” strategies achieve their goals by undermining the his will to fight, focusing on the neutralization of those key nodes, capabilities, and resources an opponent needs to retain his tactical options. In this way, modest expenditures of force can achieve disproportionate war-winning results. For example, if we understand the enemy’s logistics infrastructure in sufficient detail to enable us to identify a single point of failure in his stockpile-to-target sequence, destroying that node is a far more efficient use of force than shooting down his missiles one by one.

The Common Operational Picture

The most important element of knowledge superiority within C4ISR is shared battlespace situational awareness. This requires creating, maintaining, and disseminating a common operational picture (COP) – or set of them – in near-real time. In turn, this demands a sensor-rich tactical environment, distributed processing power to winnow, analyze, and display incoming data, and pervasive communications connectivity among participants. For naval expeditionary operations, situational awareness encompasses the entire sea-air-land battlespace, extending from the seaward approaches, across the littoral, and inland to the primary objectives. For control of the sea, the naval component will be concerned primarily with the surface, sub-surface, and air picture, whereas for Marine Corps operations ashore, the air-ground situation will be central to the COP. These views will be combined in the Single Integrated Picture (SIP), of particular importance in expeditionary scenarios





where airborne assault or defense against tactical ballistic missiles are key elements. In joint or combined multi-media warfare, maintaining the COP will be a complex, continuing process with inputs from a wide variety of sensors and reporting chains. In addition to traditional combat data links, such as Joint Tactical Information Distribution System (JTIDS), data will also be fused from satellite and remote sensors, Unmanned Air Vehicles (UAVs), Unmanned Underwater Vehicles for mine reconnaissance, manned surveillance assets, and situation reports. Battlespace sensing plays so large a role in NCW that specific “sensor operations” for “wiring” the battlespace or maneuvering to achieve favored vantage points will become an important part of the tactical repertoire.

The lifeblood of C4ISR is data – gathering it, collating it, analyzing and interpreting it, factoring it into decisions, and finally disseminating it as both useful knowledge and tactical directives to users at every command level in a form that meets their needs. Thus, every C4ISR “system” consists of three elements:

- Sensors for gathering data
- Processing, analysis, and decision nodes
- Interconnecting communication networks

NCW theorists have elaborated the requirements for each of these components in substantial detail, and a series of Fleet Battle Experiments, now under way, will evaluate key aspects of their practical implementation in realistic scenarios.

FORCenet and the Expeditionary Sensor Grid



As a goal for the future, naval warfare system architects have postulated an overarching “FORCenet” of interlocking sensors to serve both situational awareness and real-time targeting requirements for tomorrow’s littoral battlespace. This would be a system of netted, tiered sensors, ranging from a mixed constellation of earth-orbiting satellites at the top, to an “Expeditionary Sensor Grid” of remote, unattended ground and underwater sensors implanted by the local commander below. In between, large, long-endurance, unmanned UAVs at perhaps 60,000 feet will loiter over the theater to serve as

both communication relays and vantage points for down-looking sensors. Smaller UAVs and sensor-bearing manned aircraft from naval platforms would operate lower still, at “tactical” altitudes of several thousands of feet, thus supporting detailed situation assessment and real-time targeting. Naval combatants and amphibious ships off the coast and Marines on scene would contribute their own sea-level view of the encounter to the overall mix of inputs.

Transforming Data to Information

At every level from the theater commander down to individual units, the new emphasis on knowledge superiority and the vast amounts of sensor data that will become available will require commensurate capabilities for processing and assimilating information for decision-makers. Particularly for expeditionary warfare scenarios, where the land battle will be pursued simultaneously with sea control and theater air and missile defense, the COP will include so many inter-related elements and require so many disparate sensor inputs – arriving at different time intervals – that virtually all processing, fusion, and analysis functions will require extensive automation. With the need at many nodes to participate in multiple digital networks while at the same time maintaining local area situational awareness and “fighting the battle,” state-of-the-art human-systems integration (HSI) techniques will be required to assimilate, display, and respond to inputs from every direction. These techniques would use adaptive rule-based software to provide alternative interpretations of conflicting data, as well as tactical options for selection by commanders who might otherwise be overwhelmed by the torrent of information.

Networking the Force



To implement the comprehensive connectivity required for C4ISR in expeditionary scenarios, the multiple point-to-point communication links of the past will no longer suffice. Increasingly, the sheer volume of tactical information and the speed with which it has to be exchanged demands computer-to-computer communications organized as a complex of interconnecting, wide-area networks hosted on wireless line-of-sight or satellite media. In any event, the need to maintain connectivity among widely dis-

persed ground units, transport and attack aircraft, ships offshore, command echelons, logistics nodes, and other joint and allied participants demands both significant bandwidth and extraordinary flexibility.

An additional burden is created by the sensor communication requirements of the expeditionary sensor grid described previously – every node will require some means to pass its observations to tactical users or collection nodes. Moreover, maintaining secure and reliable communications in the face of constantly shifting tactical geometries, natural disturbances, and concerted enemy attempts to jam, deceive, and disrupt the C4ISR system poses a difficult engineering challenge. “Reachback” capabilities – the ability to access both rear echelon databases and human resources of relevant expertise – will also be necessary at virtually every level. One advantage of the current OMFTS concept is that the joint expeditionary force command/control function will likely be exercised aboard ship, where presumably communications connectivity and reachback capability can be better maintained than from a shore lodgement.

As originally conceived, the basic network-centric infrastructure was envisioned as the layering and interconnection of three kinds of digital networks. Known as “planning,” “sensor,” and “engagement” grids, respectively, they differ in their functional roles, data resolution in space and time, speed of response, and number of participants, as outlined here:

Grid	Function	Timeliness	Resolution	Members	Realworld Examples
Planning	Force Coordination	Minutes	Least	~1000	Global Command and Control System (GCCS)
Sensor	Situational Awareness	Seconds	Variable	<500	Combat Data Links (Link 11 / JTIDS)
Engagement	Weapons Control	Sub-second	Greatest	<25	Cooperative Engagement Capability (CEC)

Moving from the top to the bottom, each successive grid handles more finely-grained and timely information than its predecessor, from long-range planning data, through real-time target tracks and weapon assignments for facilitating engagements.

An information grid is a complex of non-real-time wide-band communication channels, largely hosted on satellite links, which provides context and background information for decision support, force coordination, logistics, and overall situation assessment. For example, satellite imagery, intelligence and order-of-battle information, and environmental data would be carried on the planning network, and the network itself would provide comprehensive reachback capability to commanders in the field. Today, the primary expeditionary planning network is the Global Command and Control System - Maritime (GCCS-M), which ties together the National Command Authority, theater and area commanders, lower level command centers, and larger individual units over both military and leased commercial communications. The Secure and Non-secure Internet Protocol Router Networks (SIPRNET and NIPRNET) are powerful wide-band adjuncts that use TCP/IP protocols for exchanging both relatively non-perishable information, such as intelligence data, geographical and geophysical information, and video-teleconferencing.



Digital data links, such as Link 11 and JTIDS, are typical sensor grids that collect, analyze, and disseminate observational data from a broad array of sensor types. These are key resources for building timely and accurate situational awareness throughout the joint expeditionary force. There will actually be a number of sensor grids – for remotely deployed battlefield sensors, underwater sensors, and satellite and/or unmanned aerial vehicle (UAV) observations, among others. While the aggregation of data from these will provide the basis for the COP – useful for early warning, cue-

ing of weapons and additional sensors, and battlespace awareness – sensor grids are not intended to convey targeting-quality data. Therefore, the timeliness and resolution requirements are not as stringent as those of the grids actually used for targeting and engagement. Virtually no participants will get all the sensor data, but a combination of “push” and “pull” access techniques will put information when and where it’s needed.

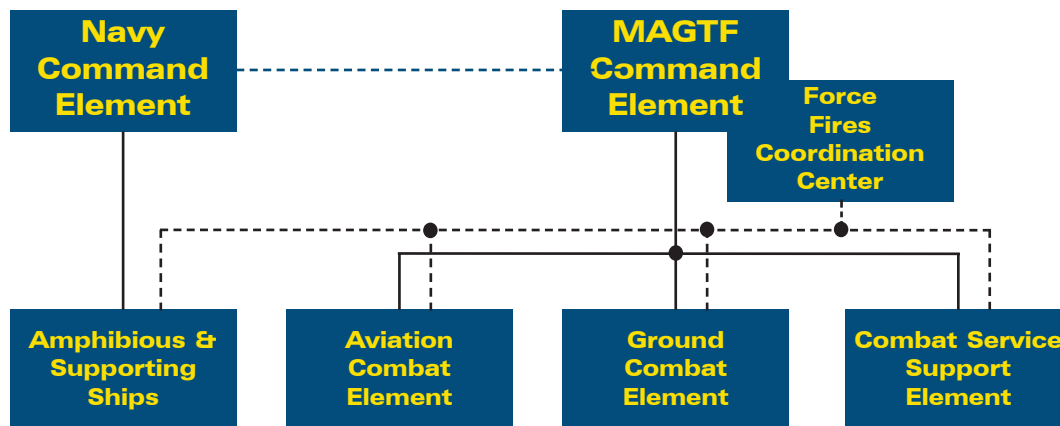


At the unit, or “shooter,” level, engagement grids will create and disseminate targeting-quality tracks for direct engagement of threats by in-area combatants. The requirements for high spatial resolution, split-second timeliness, and positive, unambiguous designation are most demanding here. As an example, the Cooperative Engagement Capability (CEC) will combine radar-level sensor data from all participants into a single, unambiguous, local-area picture that will permit tactical elements to fire on targets held by others, implement “forward-pass” techniques, and perform mutual battle damage assessments (BDA). The CEC will be a key force protection enabler, and an equivalent

joint capability will be the Joint Composite Tracking Network (JCTN), now under development on the basis of the Navy’s CEC experience.

Application to the Amphibious Task Force

A typical command and control structure for an expeditionary Amphibious Task Force can be portrayed as follows:



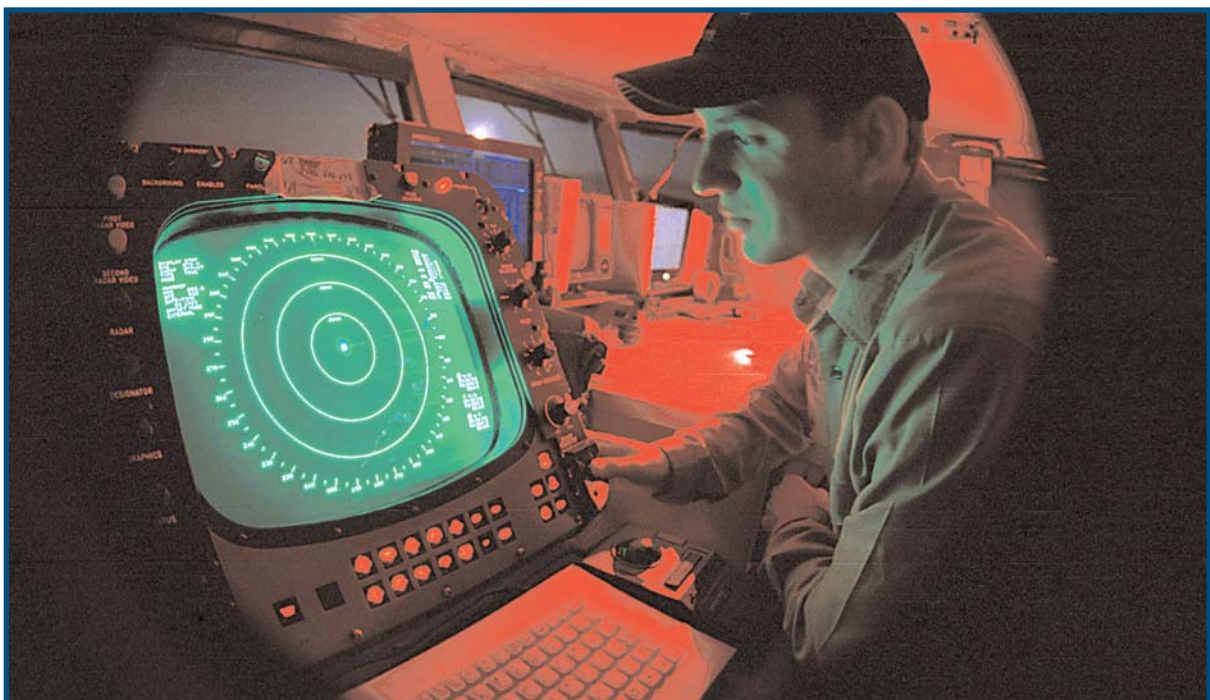
Here, the Combat Service Support Element includes supply and maintenance functions, engineering and transport services, command/control, and medical support.

This representation emphasizes the traditional hierarchy of command relationships among the aviation, ground, and support elements of the MAGTF but over-simplifies the close interaction required between the Marine Corps and Navy chains of command. One important ele-

ment of this collaboration is the Force Fires Coordination Center, which coordinates supporting fires across the entire expeditionary force by processing calls for fire, assigning targets, and deconflicting friendly fires. As such, it is an existing prototype for the kind of cross-element/cross-organizational entities that will be required increasingly to pursue joint expeditionary campaigns effectively.

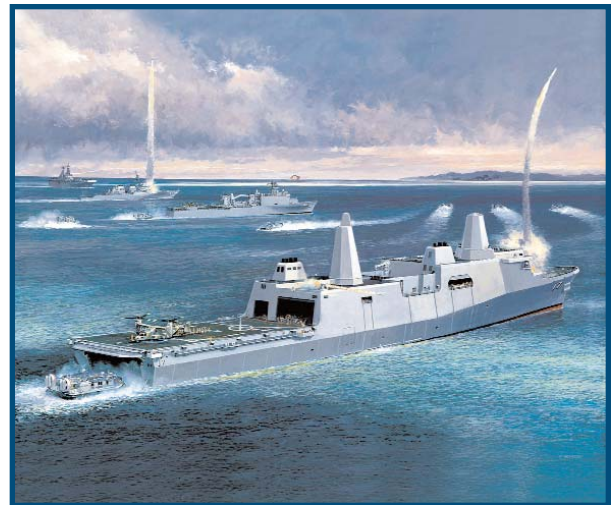
On this basis, overlaying and interconnecting the elements of this essentially hierarchical command organization are a complex of interlocking wide-area communication networks organized by function but categorized in accordance with the network-centric paradigm outlined above. Although the detailed implementation of these communication grids will vary in accordance with the operational scenario and command echelon, the following principal cross-element "affinity networks" are essential, in addition to the variety of internal networks already defined within each separate element by existing expeditionary doctrine:

- Common Operational Picture (COP)
- Fire control and targeting
- Maneuver element command and coordination
- Force-wide fires coordination (supporting arms)
- Logistics and supply
- Navy offshore coordination
- Intelligence
- Joint command/control and liaison
- Joint air and missile defense



Each grid will have its own subscriber community, and individual nodes – command centers, aircraft, ships, small ground elements, etc. – will in general be multiply-connected for gaining access to the specific tactical information each needs and for providing local information to others. For each node, a combination of user “pull” and supplier “push” techniques will be used to regulate traffic flow and minimize information overload. Selected real-time tactical channels will carry voice or even video-teleconferencing links, but the great preponderance of information will be exchanged and accessed via computer-to-computer communications.

In a typical scenario, the COP – or local-area subsets of it – will be readily accessible to tactical users at all levels as the basis for force-wide, near-real-time situational awareness. It will provide a common geographical framework within which virtually all expeditionary warfighting and support functions can be planned, implemented, displayed, and assessed. The COP will be created and updated continuously by analyzing, correlating, and fusing all-source sensor and friendly self-reporting data with satellite observations and geophysical and environmental inputs. It will display both own-force and enemy positions with sufficient timeliness and accuracy for reacting quickly to enemy countermoves, exploiting emerging opportunities, and coordinating supporting arms.



Targeting-quality information will be shared over a mix of engagement nets at higher data rates. For air and missile defense over the littoral battlespace, ships, tactical aircraft, and both air- and ship-borne surveillance and tracking sensors will be netted to coordinate target assignment, real-time engagements, and BDA. For supporting fires against land targets, a similar grid – with inputs derived from a variety of sensors – will identify and geo-locate both fixed and moving targets, with particular emphasis on “pop-up” and time-critical threats such as mobile missile launchers and enemy armor. The resulting shared targeting picture will be available to both the shipboard Naval Fires Control System (NFCS) and the Marine Air Command and Control System (MACCS) to allocate naval gunfire and close air support among competing target priorities.

With the prevalence in OMFTS and STOM of rapid simultaneous thrusts toward inland objectives, coordination among the combined arms of each maneuver element and with adjacent lines of attack demands more than a hierarchical command/control approach. In comparison to the traditional vertical command structures already in place within the aviation, ground,

naval, and support elements, horizontal peer-to-peer coordination and supporting communications become even more important. Thus, ground combat units must be able to interface directly with fire support and aviation, logistic elements with ships offshore, and forward command posts with each other. Again, an interlocking grid of special-purpose “affinity” networks will be established to facilitate the unit-level “self-synchronization” required to exploit emerging opportunities and to achieve rapid decisiveness. Eliminating the need for “up-and-over” communication among adjacent and mutually supporting combat elements enhances both speed of reaction and the multiplier-effect of initiative and on-scene tactical awareness.

The participation of other joint or international forces – or even non-governmental organizations (NGOs) in the case of humanitarian missions – creates another dimension of coordination and communication requirements. Not only will technical and procedural protocols need to be established, but a multiplicity of security and political issues come into play that may need to be adjudicated much higher in the chain of command and thus require special accommodation in the overall command/control infrastructure. With naval expeditionary forces deployed increasingly as joint force enablers, the expeditionary C4ISR “system of systems” must be capable of accommodating the subsequent joining up of follow-on joint-force or NGO units, or for relinquishing local command seamlessly to higher echelons when they arrive on scene. This entails designing a command/control infrastructure that can function both as a stand-alone entity and as sub-element of a much larger system. The engineering challenges are formidable, but solutions are achievable.

Technology Challenges in Implementing Expeditionary C4I Capabilities

Significant progress has been achieved in implementing a rudimentary C4ISR infrastructure for supporting future expeditionary warfare. Combat data links, GCCS-M, SIPRNET and NIPRNET, the shipboard wide area network (SWAN), and the Aegis command and display system as situational analysis tool have all have proven their worth in operation and appear ready to be incorporated into a new synthesis. Moreover, the Naval Fires Network is under development to integrate the planning and execution of supporting fires, and many aspects of that functionality have been demonstrated. Several platforms specifically intended for expeditionary roles – notably the San Antonio (LPD-17)-class amphibious assault ship and the Future Surface Combatant Program: DD (X) destroyer and CG (X) cruiser – are being designed with Total Ship Computing (Photo R) Environments for seamless participation in network-centric operations. Additionally, the Navy Department’s Information Technology for the 21st Century (IT-21) program is funding a massive upgrade of the computational infrastructure needed to bring both ships and shore stations into the information age. IT-21 will upgrade processing and display capabilities, facilitate computer-to-computer networking for process re-engineering, and enhance broadband digital communications to ships at sea – all within a common hardware and software environment.

Moreover, the Navy Warfare Development Command has made significant progress in organizing a series of “Fleet Battle Experiments” (FBEs) to evaluate several key NCW ideas. The FBEs are designed to explore future command/control concepts and technologies through operational experimentation, while providing a venue for rapid prototyping and warfighter feedback. While none of the nine FBEs to date have attempted a full-fledged implementation of

a network-centric architecture, key C4ISR elements and several expeditionary warfighting concepts, such as OMFTS itself and “Ring of Fire” – central, coordinated direction of land-attack

FBE	DATE	Fleet	Operating Area	Concepts / Scenarios Evaluated
ALPHA	3/97	THREE	Southern California	OMFTS; Central coordination of land attack fires
BRAVO	9/97	THREE	Southern California	As above, with JTF targeting of GPS-guided munitions
CHARLIE	5/98	TWO	Atlantic Coast	Theater Air & Missile Defense; area coordination
DELTA	9/98	SEVEN	Korean Theater	Counter-SOF; counter-fire; linking with Army fires
ECHO	3/99	THREE	Northern California	Asymmetric Urban Threat; multi-dimensional warfare
FOXTROT	12/99	FIVE	Arabian Gulf	Assuring access to littorals; SLOC protection
GOLF	4/00	SIX	Mediterranean	Time critical targeting; theater/air missile defense
HOTEL	8/00	TWO	Gulf Coast	Mine Countermeasures; sea-based fires
INDIA	6/01	THREE	Southern California	Naval Fires Network; wireless networks; littoral warfare

fires – have been demonstrated in the series so far:

Despite this continuing progress, significant technological hurdles remain in key areas:

- Reliable wireless connectivity for adaptive networks
- Battle space sensors and sensor communications
- Multi-sensor fusion and correlation
- Human-machine interface for display and decision-aiding
- Combat identification
- Automated multi-level security
- Adapting to non-conventional scenarios and missions

With such heavy emphasis on network-centric concepts of operations, future expeditionary initiatives can only be as robust as the communications infrastructure that supports them. Moreover, the more complex and intricate the required network functions – the more data that has to be moved in careful synchronism – the more vulnerable the system becomes to information denial. With the complex of interconnecting networks so tightly connected to platforms and weapons in all its parts, the easier it becomes for failures to propagate through the structure. Expeditionary campaigns will not take place in a totally benign environment. Not only will natural interference and battle damage undermine sensor performance, but likely adversaries will be using every tool of jamming, deception, and misinformation to bring the supporting networks down. Communication and information technology spreads so quickly around the world that likely opponents will have access to techniques and hardware of virtually the same sophistication of our own. At this juncture, it seems unwise to depend heavily on enjoying a significant technological edge over the enemy.

No matter how much progress is made in communication system technology over the coming decades, sensor communications will remain a near-intractable problem, if only because of the sheer number of entities – sensors, platforms, fusion nodes, guided munitions – that will

need to be linked together in near simultaneity to provide a “God’s-eye” view of the battlespace. These capabilities will, in turn, be heavily dependent on a multiplicity of vulnerable line-of-sight and satellite links that demand sophisticated transmit/receive equipment, intricate mechanisms for routing and distributing information, and large spectrum allocations. To be sure, there are promising techniques for error correction, alternate routing, and fault tolerance, but they all require significant system “overhead” in the form of higher data rates, back-up channels, and processing capacity. It is easy to reach the point where this additional overhead – intended to make the system invulnerable – simply overwhelms the useful information.

These demands on sensor communication are exacerbated by increasing dependence on multi-sensor fusion among elements of the sensor grid to minimize targeting and situational uncertainty. Simply fusing processed contact reports will not sufficiently minimize the inherent ambiguities. As in today’s rudimentary Cooperative Engagement Capability (CEC), access to actual sensor outputs – essentially raw data – will be necessary at the fusion node to take full advantage of all the sensor clues – in waveform, spectrum, and timing – necessary for unambiguous target identification and geolocation on the basis of noisy and uncertain inputs.

This demands at least an order of magnitude more bandwidth for a large subset of the sensor communication channels, to say nothing of the enormous computational capacity needed to execute fusion and correlation algorithms on a time scale brief enough to satisfy latency – time required to process network information – requirements. Moreover, the inherent complexity of expeditionary operations – notably Expeditionary Maneuver Warfare – and the need for comprehensive situational awareness will generate orders-of-magnitude-more tactical data than has been available in the past. Until automated means are available to order, integrate, and display this material in forms that facilitate understanding and aid decision-making, information overload will become a limiting factor at every level.

Combat identification – the ability to tell friend from foe – is an essential aspect of knowledge superiority, particularly in fluid combat situations where multiple, independent thrusts may interpenetrate hostile territory simultaneously. With decreasing dependence on conventional IFF (Identification Friend or Foe) systems that use active query-and-response techniques, situational awareness – “guessing what [or who] is at the other side of the hill” – becomes the primary mechanism for combat identification. This in turn places heavy demands on the comprehensiveness and geolocation accuracy of the COP, particularly for friendly forces, and it essentially requires an automated real-time position-reporting scheme for friendly units, perhaps by impressing GPS coordinates on each individual’s network communications.

Needless to say, the operational security aspects of this approach will have to be closely monitored, and the requirement for multi-level security will become a key factor in handling and protecting a wide range of sensitive information. While today’s systems – such as RADIANT MERCURY – still require a “man-in-the-loop” to forestall unauthorized distribution of special-access information, the new volumes of tactical data associated with expeditionary campaigns will demand new levels of automation or a less cumbersome security apparatus.

Finally, there is a key challenge associated with the changing nature of warfare itself. Although today’s planners acknowledge the large variability of potential expeditionary operations – and the flexibility required to deal with it – a significant emphasis remains on supporting large-scale conventional campaigns reminiscent of the Gulf War or postulated for the Korean peninsula. Many canonical scenarios envision the use of naval expeditionary power to

repel invading forces from friendly territory by seizing “centers of gravity” or massing precision fires against a large, but denumerable, set of discrete targets.

However, many military futurists have questioned the actual probability of such events even now. To these theorists, the preponderance of future conflict seems much more likely to resemble today’s insurrections, brushfire wars, and organized terrorism, pitting ideological fac-

tions and “non-state actors” against each other and against established governments. These adversary forces will be organized irregularly, dispersed widely within indigenous populations – often in an urban context – and heavily reliant on exploiting asymmetries against more powerful enemies. In essence, armed conflict in the 21st century will much more closely resemble the Vietnam War than Desert Storm – there may well be no “front line.”



If our expeditionary concepts of operation de-emphasize these alternative scenarios, there is a very real danger that the hardware and software we actually deploy may be only minimally useful against many real-world emergencies that actually materializes. For example, if the capabilities of the expeditionary sensor grid are optimized for discrete moving targets and large force concentrations, the system may simply overlook many key enemy activities of greater importance in unconventional conflict. For the most part, our sensors will need the capability to detect and identify much more dispersed, ill-defined, and better-concealed threats. The future battlespace, in fact, may offer no targets in

today’s sense, even while the adversary is still there, controlling the ground. Thus, in developing broad-spectrum expeditionary capabilities for the 21st century, the entire range of likely contingencies needs to be factored in.

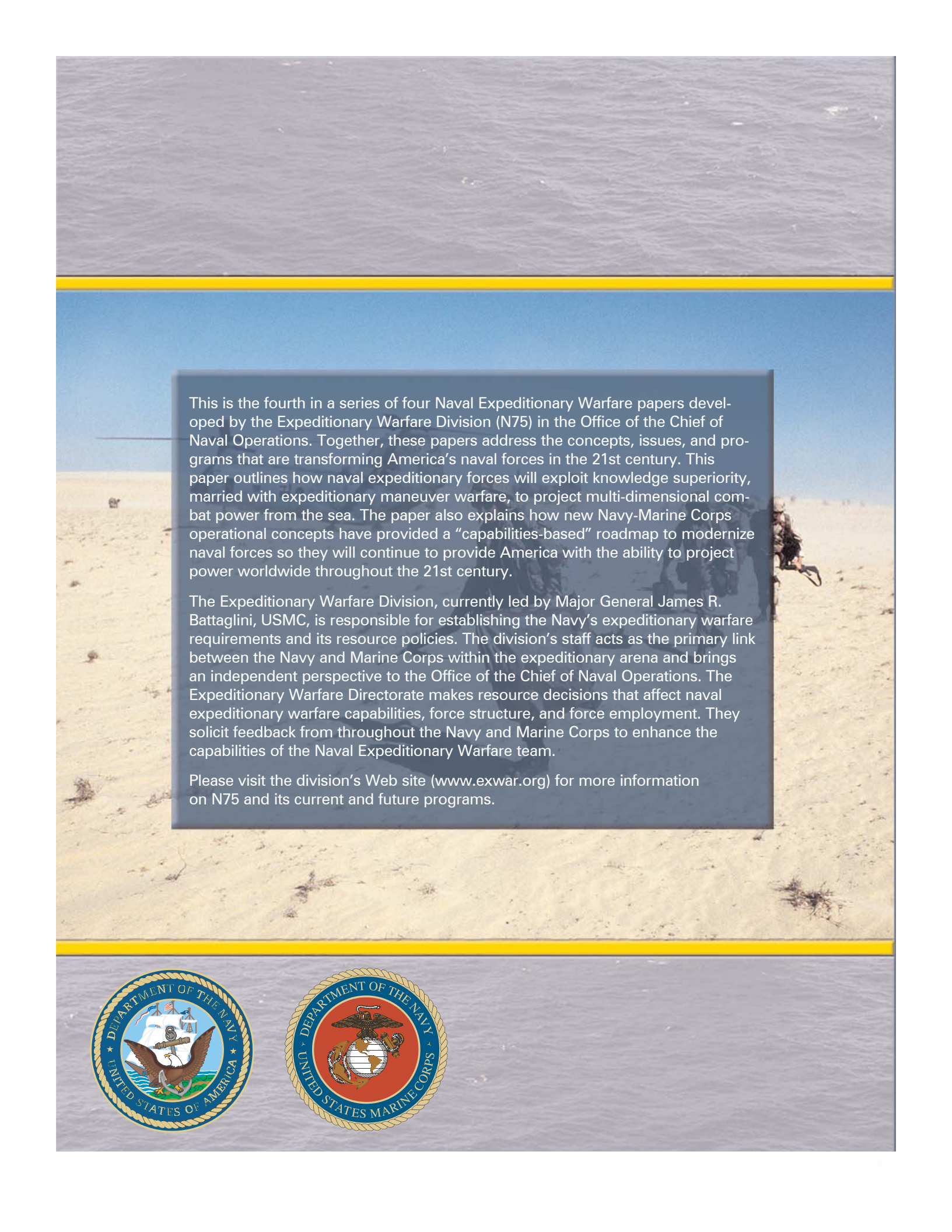
Back to the Future

Achieving the “Full Spectrum Dominance” predicated in Joint Vision 2020 requires two key enablers: information superiority and continuous innovation. These same enablers become even more crucial for expeditionary maneuver warfare, where the complexity of the battlespace, the challenge of assuring access, and the coordination of dispersed forces all place huge demands on the full spectrum of C4ISR capabilities. In turn, gaining and exploiting a

decisive knowledge advantage makes possible not only the execution of innovative concepts of operation but also confident, real-time tactical improvisation that exploits emerging opportunities and keeps adversaries uncertain and off balance. These basic ideas are not new. Nimitz exploited information superiority at Midway; Napoleon innovated continuously. But no previous era has offered such an embarrassment of technological riches applicable to transforming



expeditionary maneuver warfare so fundamentally. Significant technical innovation will be necessary to achieve fully the larger vision described above, but our progress to date has been impressive, and its pace has been increasing and necessary.

The background of the slide is a photograph of a sandy beach under a clear blue sky. In the distance, several soldiers in camouflage gear are visible, some standing and some in a crouched position. A thick yellow horizontal stripe runs across the middle of the slide, separating the top image from the bottom image.

This is the fourth in a series of four Naval Expeditionary Warfare papers developed by the Expeditionary Warfare Division (N75) in the Office of the Chief of Naval Operations. Together, these papers address the concepts, issues, and programs that are transforming America's naval forces in the 21st century. This paper outlines how naval expeditionary forces will exploit knowledge superiority, married with expeditionary maneuver warfare, to project multi-dimensional combat power from the sea. The paper also explains how new Navy-Marine Corps operational concepts have provided a "capabilities-based" roadmap to modernize naval forces so they will continue to provide America with the ability to project power worldwide throughout the 21st century.

The Expeditionary Warfare Division, currently led by Major General James R. Battaglini, USMC, is responsible for establishing the Navy's expeditionary warfare requirements and its resource policies. The division's staff acts as the primary link between the Navy and Marine Corps within the expeditionary arena and brings an independent perspective to the Office of the Chief of Naval Operations. The Expeditionary Warfare Directorate makes resource decisions that affect naval expeditionary warfare capabilities, force structure, and force employment. They solicit feedback from throughout the Navy and Marine Corps to enhance the capabilities of the Naval Expeditionary Warfare team.

Please visit the division's Web site (www.exwar.org) for more information on N75 and its current and future programs.

